IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
NORFOLK DIVISION

CENTRIPETAL NETWORKS, INC.,	)	
	)	
Plaintiff,	)	
v.	)	Civil Action No.:
	)	2:18cv94
CISCO SYSTEMS, INC.,	)	
	)	
Defendant.	)	

TRANSCRIPT OF VIDEOCONFERENCE BENCH TRIAL PROCEEDINGS

Norfolk, Virginia
May 7, 2020

Volume 2A
Pages 165-249

BEFORE: THE HONORABLE HENRY C. MORGAN, JR.
United States District Judge

Appearances: (Via Zoomgov Video)

KRAMER LEVIN NAFTALIS & FRANKEL, LLP
By: PAUL JOSEPH ANDRE
Counsel for Plaintiff

DUANE MORRIS, LLP
By: LOUIS NORWOOD JAMESON
Counsel for Defendant

I N D E X

E X H I B I T S

P R O C E E D I N G S

(Proceedings commenced at 10:07 a.m. as follows:)

COURTROOM DEPUTY CLERK: In Civil Action No. 2:18cv94, Centripetal Networks, Inc. v. Cisco Systems, Inc.

For the plaintiff, Mr. Andre, Mr. Noona, are you ready to proceed?

MR. ANDRE: We are, Your Honor.

COURTROOM DEPUTY CLERK: For the defendant, Mr. Jameson and Mr. Carr, are you ready to proceed?

MR. JAMESON: We are, Your Honor.

THE COURT: All right.

Lori, do those earphones work on this technology?

MR. ANDRE: Your Honor, this is testing of the ear phones. Do they work?

THE COURT: Just a second, I'm trying to -- I can't hear you.

MR. ANDRE: Can you hear us okay? This is Paul Andre speaking.

THE COURT: Yes.

MR. JAMESON: Your Honor, this is Woody Jameson. I'm assuming it's okay?

THE COURT: Yes. All right. Are you ready for your opening statements?

MR. ANDRE: We are, Your Honor.

THE COURT: All right. Well, I'll hear first, of course, from the plaintiffs.

MR. ANDRE: May it please the Court, Paul Andre for Plaintiff Centripetal Networks. May I proceed?

THE COURT: Okay.

MR. ANDRE: Good morning, Your Honor. Steven Rogers formed Centripetal Networks --

THE COURT: I'm sorry, these are not working. Or this one. Sometimes one of them works, the other one doesn't.

All right. Go ahead.

MR. ANDRE: Testing 1, 2, 3. Does that work?

THE COURT: No.

MR. ANDRE: It's not working?

THE COURT: Maybe they just don't work with this technology.

MR. ANDRE: Testing, testing, testing?

THE COURT: No.

COURTROOM DEPUTY CLERK: Say something.

MR. ANDRE: Testing. Testing, 1, 2, 3.

COURTROOM DEPUTY CLERK: I can turn up your volume.

(Pause in the record.)

THE COURT: Try it again.

MR. ANDRE: Testing, 1, 2, 3. Testing, 1, 2, 3.

THE COURT: Did you turn it up, Brandan?

(Pause in the record.)

THE COURT: All right. Try it again.

MR. ANDRE: Testing 1, 2, 3? Testing 1, 2, 3? Audio Test 1, 2, 3?

THE COURT: I only misheard one word yesterday...

Try it again.

MR. ANDRE: Testing 1, 2, 3.

THE COURT: No. Okay. Well, as I said, I only misheard one word yesterday, so let's just go ahead and hope it works.

MR. ANDRE: I'm optimistic, Your Honor. We'll give it our best shot.

THE COURT: All right.

MR. ANDRE: May I begin?

THE COURT: You may.

MR. ANDRE: Thank you, Your Honor.

Steven Rogers founded Centripetal Networks in 2009. Working from his basement in Vienna, Virginia, he thought he had a better idea, a way to solve the cybersecurity problem that was affecting the country at the time. Around 2009, Mr. Rogers had about 40 years of experience in secure communications. He had worked on secure communications in the Air Force for the AWACS airplanes and the Air Force One. He worked at defense contractors working on secure communications as well. And when he saw the looming problems in 2009, what was happening in

cybersecurity, he thought he might have a better solution, a new way of doing something.

The scope of the problem really started magnifying in 2009. The slide that's on the screen now, this is a threat assessment that was done by the Office of Naval Research. I will show the actual graph. This was put out in the 2009/2010 time period. The red line indicates the threat that was coming into the United States, into our infrastructure. The yellow line demonstrates the capacity to handle that threat. This was a motivating factor into Mr. Rogers' thought process. What could he do to bring the red line up to meet the yellow line to match the threat?

The problem with the old systems were that you had an initial line of defense at a firewall that was easy to overcome. Once it got into the network, the routers and switches and the network infrastructure allowed the virus to come in. The primary point of defense was around the endpoint.

I think everyone can remember looking at antivirus products from McAfee and Symantec. And what they were focused on was making sure the virus or malware didn't get to your computer. They would actually install the malware on the laptop or the desktop. That's where they tried to stop it. So when they started looking at the network, they took that same strategy they used on the endpoint and tried to apply it to the network. What Mr. Rogers' grand idea was, was to make the

network smart. Don't let the bad guys get into the network. Centripetal's solution wanted to make the network devices smarter. That was the key.

If you look at the slide, you can see as the package goes through each aspect of the network it gets inspected. It gets at the firewall, it gets inspected at the router, it gets inspected at the switches. So not only do you have your end-point protection that you normally have, but you have protection, smart protection, at each stage of the network transport layers. So you have the files, routers and switches being fed threat intelligence. The threat intelligence focused on who was out there trying to attack you instead of what was trying to attack you. And this was a key derivation of how cybersecurity, what was done.

Mr. Rogers used his experience, his 40 years of experience in secure communications and applied that to a new field, cybersecurity. As a result, he invented essentially a new market. It was a new paradigm shift in how security was going to be done.

Now I want to talk a little bit about the history of the company. As you can see on the slide, it was founded in 2009. It was very motivated to find a solution by the Office of Naval Research proposal in which they got it and they said this is a proposal to protect our nation. Shortly thereafter, the Department of Homeland Security put out another proposal. They

called it the Grand Challenge. And both of those challenges Centripetal answered. They also got a CIA innovation grant, and as they started working on this project and coming up with solutions -- and it wasn't fast, it took them nearly four years to come up with the first solution of full-time work to try to do this new technology -- they started filing their patents. In late 2014, December 2014, they finally had their first product that was ready for launch. It was the RuleGATE product. So December '14 was their first sale, and they have been selling products ever since then.

Now I mentioned the Office of Naval Research challenge, the proposal that they put forward. And on the Industry Day, the director put out the problem that was existing in the country at that time. And this was in 2010.

We go to the next slide, you'll see the graph that was, what we used for our first slide. You see the red line is the threat that the government foresaw. The black line was the capacity. This is what the United States government was looking at and determined that we don't have the capacity to do it. If you look at the bottom box in the bottom of the yellow box, talked about "Signature-based defensive hosts, antivirus and network firewalls are ineffective. We need new ways to frame, understand and reverse these trends."

This was a large motivating factor for the employees at Centripetal. They saw this, they said we've got to meet the

threat line. So the Department of Homeland Security issued a Grand Challenge around the same time. They called it the NS2R goal; that is, the mission to secure, protect and defend U.S. Internet infrastructure from extreme cyberattacks. This was the challenge that was put out there. Centripetal won the grant. They participated in the challenge and they were awarded a million dollar grant to begin this research.

As the Department of Homeland Security stated, "Centripetal Networks will research, develop a network protection system capable of providing a network survivability, recovery and reconstitution service requested by the Department of Homeland Security. The NS2R will help the DHS" -- Department of Homeland Security -- "achieve its mission to secure, protect and defend U.S. Internet infrastructure."

This was proof of concept that Mr. Rogers' original idea was a good one. The people at the Department of Homeland Security saw the potential. They recognized that this was a new paradigm. This was a new way of solving the security problem.

From that, Centripetal accelerated their development. They started getting more funding, and essentially, as I said they launched the RuleGATE product. RuleGATE is an appliance that can sit in the network, different places, it is fed threat intelligence, and it is there to make the network smarter. To keep the bad guys out of the network altogether.

THE COURT: What you're saying is the new concept, the

concept of rules that can be applied anywhere in the network? Is that the new concept?

MR. ANDRE: Rules and policies, that was the first concept. Being able to do rapid rule swapping, putting new rules into the network and basing those on current threat intelligence. What's very important about Centripetal's concept is that you take rules and policies and put them into the network devices. You can update those on the hour, within a half hour, within minutes. The threat that Centripetal saw was the fact that the enemy, the terrorists, the cyber terrorists, were getting more sophisticated. It just wasn't the kid in the basement trying to hack into the system. These were organized crime, these were State actors. They were countries, our adversaries, trying to hack into our systems. So you had to be able to change the rules and have dynamics policies at the drop of a hat. You had to -- as soon as you got new threat assessments, as soon as you got chatter and you knew something was out there, you had the ability to respond quickly.

So if you look the first set of patents that we talk about today, that's what those are about. They are rapid rule swapping. As Your Honor noted, can't just keeping piling rules on top of rules. You have to have new rules. You have to be able to swap out rules and you have to do it without interrupting the flow in any noticeable way. You have to be able to make the actual devices in the network smart. The

routers and switches. You have to update firewalls. That's the key. You have to have policies that contain the rules that are dynamic. The dynamic policies are very important here. Because if you have a stale policy, that's how the adversaries get in.

We'll talk about each of those patents in a few minutes. But when RuleGATE was launched, it was heralded as something now. Centripetal started receiving awards and recognitions from this new concept. I mean, you'll hear Mr. Rogers talk about this, he's our next witness when we finish our closing -- I mean our openings.

So this was a new, as I said, a new way of thinking about security.

They also started getting customers. The list of some of the people in the Department of Defense, Homeland Security, defense contractors, universities, they started making inroads. They started getting sales. The first year of sales in '15 was good, good for a startup company, and in '16 it doubled. In '17 it was doubling again. But then something happened. Everyone started looking at Centripetal and saying that's a good idea.

Now, when you're a small smart-up company, you try to make partners with bigger companies. That's what you do. Sometimes big companies just take the technology and do not partner with you. That's the reason Centripetal filed patents. One of the only things small companies can do to protect

themselves in the marketplace when they're starting out with a new way of doing things is to patent it. And Centripetal, because Mr. Rogers had started up several companies very successfully, he knew that you had to protect your technology.

So in this case, in this trial, we have five patents that we're talking about, and each one of these patents have a different aspect of using intelligence to protect a network. I'll start with the '193 patent. That's going to be the first one you hear about. This is a patent that's going to provide visibility based on traffic in other networks, and it can drop inappropriate packets. Now, if you look at the animation you saw yesterday from Dr. Medvidovic, you saw there's a set of rules on the routers and switches, and it applies those rules to determine whether or not the package is allowed to go forward or if it's dropped. Now, that's a great first start. You have a package, a packet that's coming through, these routers and switches, and if they violate the rule, if the rule says drop it, drop it. If it says it's okay, it's okay.

This technology is found on Cisco's switches. And you'll see that when you look at the Cisco switches, these are the Catalyst 9000 switches with ETA. Those switches can forward or drop packets. It's also found on Cisco's routers. The routers have the same software, the same operating system as the switches, and they operate in the same way when it comes to packets. They can forward or drop the packets.

Now, yesterday you heard in Cisco's tutorial that they don't do that. They don't forward or drop. They don't drop, they just forward it on and they do it after the fact. I think you may have remembered that, Your Honor. After the fact. They let the bad guys in and do it after the fact. We heard that a lot. But that's not what their documents say. That's not what their technology does.

This is a Cisco document describing the Catalyst switch. "The 9000 switching advanced security capabilities." If you look at the bottom of that slide it says "Detect and stop threats, exclamation point." That's what the Catalyst can do. It can detect and stop threats. "In a security designed to work together. Simple security complexity keeps business more secure, makes IT more productive."

Yesterday in the tutorial you heard that the Catalyst switch just forwards packets, they don't detect. They don't stop. They say after the fact they try to figure it out. We heard that a lot. We'll show you in this trial numerous documents, Cisco's documents, which use Cisco's testimony, Cisco's source code that shows that the switches and routers in this case have the ability to either forward or drop packets based on those rules that are on those switches and routers. If you look on the, just on the bullet points on the right, "during". There's policy enforcement analytics, Encrypted Traffic Analytics. They have full NetFlow-based behavior

analytics. They have rapid threat containment. So the information provided in the tutorial that the switches and routers just forward things on and don't make this type of determination whether to drop or forward is going to be contradicted by a ton of evidence in this case.

The next patent that we're going to talk about is the '806 patent. This is what we call the rule swapping patent. What happens here are rule sets are preprocessed up in the Cloud, and the packets are processed in accordance with these rule sets. And you saw this in the tutorial yesterday by Dr. Medvidovic that when the -- go to the next slide, please -- when you have the rules being preprocessed up in the Cloud and you need to swap out the rule set for Rule Set 2, it can do it very quickly. Very rapidly. It's called rapid rule swapping. And it has to do this in such a way that traffic is not visibly disrupted. You have to be able to swap out those rules very quickly. This was a key aspect of how this could be used. Because one thing you cannot have is when you change the rules and you have to update on a very regular basis, you cannot have disruption in traffic. No one will buy it. So you have to be able to do a rapid rule swapping and preprocessing rules beforehand. So you need something up in the Cloud preprocessing the rules and then doing the rule swapping.

They used this type of technology, Cisco used this type of technology on their firewalls, switches and routers.

We'll talk about that in great detail with Dr. Mitzenmacher, who will be a witness hopefully later today.

The '205 patent is the third patent we'll be talking about, and this is the, we call it the Dynamic Security Policy patent. Now, it's important for this patent that you update the Dynamic Security Policy with threat intelligence. Efficiently analyzes large amount of network traffic. Now, if you remember from the graphic yesterday in the tutorial, what happens here is you have, up in the Cloud, a policy manager, and you need to keep that Dynamic Security Policy dynamic. Policies change like rules change. So you have to have a Dynamic Security Policy. The rules are within the policy. So rules are triggered and then you have a policy that you have to have that say what should we do if these rules are triggered? So you have a set of rules, and then a policy that tells how you're going to respond when these rules are violated. And that policy has to be dynamic. That's key. Has to be a dynamic security policy.

Now the '806 and '205 patent, in order to have this type of rule-swapping and the dynamic policy, they interact with what Cisco calls the Digital Network Architecture, or DNA Center. So the DNA Center, the Digital Network Architecture, is sitting up in the Cloud, and it constantly is in communications with the routers and switches to allow them new rules that come in, when intelligence comes in, that these rules may be updated. They can do so and they can do it at any time of the day, 24

hours a day. This is a 24/7/365. So this is something that is -- the DNA center kind of helps with the intelligence in making it operational. Operationalizing the intelligence is key.

THE COURT: Tell me again what the DNA Center is.

MR. ANDRE: They call it the Dynamic Network -- Digital Network Architecture. The center itself is another box. It's up in the Cloud. They have several different components. And what it does, it takes intelligence from around the world. These companies subscribe to threat intelligence feeds from multiple third-party vendors. And you take all the intelligence you can receive, who are the bad guys out there, what are the bad guys doing, and then you need to process it. You need to make sense of it. You need to make rules of from it. You need to change policies based on it. And then you feed that information down to the routers and switches so they're smart. And the firewalls. So you have to, the DNA Center does it for the routers and switches. So they call it DNA because it's the Digital Network Architecture and they make the symbol like a biological, like a strand of DNA, it's a nice marketing ploy, but it has nothing obviously to do with DNA. This is about the Digital Network Architecture. A new architecture that was introduced in 2017 by Cisco.

Now, the switches with the DNA infringe '806 and '205 patent. Same with the routers with the DNA. Same principle

applies. But with the firewalls, they don't use the DNA system. The firewalls are different structures. They use what's known as -- go to the next slide, please -- this is actually a DNA strand. I'm sorry.

The DNA Center is, as you can see, Your Honor, they have a DNA Center dashboard, the appliance, and then the network devices that feed into it. So this actually shows you the DNA Center that is actually doing the threat intelligence up in the Cloud and then sends down to the routers and switches. And you'll hear a lot about the DNA Center and the DNA solution from Dr. Mitzenmacher later today, hopefully.

But then the firewalls, they don't interact with DNA, they interact with what they call the Firepower Management Center, the FMC. So this is the brains for the firewall to allow it to update the rules and update the policies. So they abbreviate with a little fire symbol. It's FMC. That's the Firepower Management Center. This updates the Firepower and the ASA firewalls. So they sit before that.

And if you look at the next slide, you'll see how Cisco describes its FMC, the Firepower Management Center. You see the third-party sources on the left? That's the threat intelligence feeds. So they get all this threat intelligence that comes in from all these third parties from around the world, all these security companies who you can pay for this intelligence feed. There's entire companies that rely, that,

their whole source of business is coming up with intelligence feeds. It feeds it into the Firepower Management Center, and the Firepower Management Center uses something called a threat intelligence director to make sense of all those feeds, and then they update the rules, the rule sets and the policies down on the firewall.

So the next patent that we'll be discussing is the '856 patent. This is called the encrypted traffic patent. Now, this patent is concerned about detecting network threats in encrypted traffic using the threat intelligence that we were talking about. And what it does, it identifies the encrypted packets corresponding to network threats based on the unencrypted data. Your Honor had a lot of questions about this yesterday. Looking at the unencrypted information in the header and the source address and all that kind of stuff and a lot of other things about the packet, all the things that are unencrypted, you can make inferences on what the encrypted packet portion, the payload is doing, or what it wants to do. So you determine the threat of the encrypted portion by looking at the unencrypted portion, and then based on those threats, you can route the identified packets to a proxy system. I believe Cisco's tutorialist called it, you can route it to a proxy server. And in its tutorial I think that's what he said. And that's exactly right. If you detect something that you think that the payload might be -- the encrypted payload might be a

threat based on these indicators, you don't let it go through, you stop it, you send it somewhere else. You send it to a proxy.

Now, you saw this in the tutorial by Dr. Medvidovic. As documents are coming through, the routers and switches are going to look at both unencrypted packets and encrypted packets, and based on the information from the unencrypted aspects of it, it's going to make a determination whether or not it needs to route it to a different proxy.

Now, if you look at how this is included in Cisco's systems, the switches interact with something called StealthWatch. And there's a constant feed of information from the switches to StealthWatch. StealthWatch is getting third-party feeds, the intelligence feeds, and StealthWatch then sends its information to something called the Identity Services Engine the ISE. And the ISE then can given information to the switch and say this is something that we're seeing, it looks like it could be a problem, and take remedial action. Reroute it quarantine it. Do something with it.

The switch to the routers operate just like the switches. You have the router feeding information to StealthWatch, StealthWatch and ISE interact back and forth, and then ISE tells the router what to do and sets up the policies as to whether it should be redirected or not.

One of the things you'll notice is these little orange

and purple buttons with Encrypted Traffic Analytics and Cognitive Threat Analytics. The Encrypted Traffic Analytics was a technology that was introduced in 2017 by Cisco, and we'll talk a lot about Encrypted Traffic Analytics. It's throughout their entire security system in their network at this point. As you've heard, if you can't deal with encrypted traffic, you're not in business.

THE COURT: If you can't what?

MR. ANDRE: If you can't deal with encrypted traffic, if you don't know how to deal -- if you cannot reconcile the encrypted traffic, you're out of business. There's so much encrypted traffic now, the vast majority of traffic on the Internet is now encrypted. And you'll see that in Cisco's own documents and you'll see the importance of the ETA, the Encrypted Traffic Analytics, is to Cisco's entire infrastructure.

If you look at how Cisco describes its products, you'll see this is another Cisco technical document, the schematic they have on this document as exactly as we put into our animation. You see the switches down at the bottom, you see it interacting with the StealthWatch, with the CTA, StealthWatch going back and forth with the Identity Services Engine, the ISE, and then you see the ISE communicating down to the switches. And it says the Change of Authorization, the COA. That's when the switches, these packages are not authorized. Reroute them.

And this is all happening, Your Honor, at light speed. This is happening multiple times, if not a day or an hour, per minute. It could be multiple times within five minutes. You have to stay on top of the criminals.

The last patent we'll be talking about is the '176 patent. We call this the correlation patent. So what this patent does, it correlates packets in the network. As a packet comes into a router or switch, it creates a log of that packet. When it exits on the other side of the router and switch going into a network, it does another log. When a packet leaves the network, like your private network going back out in the Internet, it logs it when it enters a switch and it logs it when it exits the switch. It leverages these log entries to perform a correlation, and what the correlation is, is a way to try to figure out if the packets are used to identify malicious entities. So if you see a certain type of information on these logs, you might think, hang on a second, these packets are doing something funny. And by correlating them going in and out of the network, you can make a determination whether or not this is malicious activity. In other words, if a criminal goes and gets into your network and says send me all your passwords or I want all your banking information, by correlating what's happening when it comes in and when it comes out of your network, you can actually make a determination whether or not that is a malicious entity that's doing that.

We saw this in the animation yesterday where the packet was coming in and Log Entry 1 would happen. It would leave the router and switch you have another log entry. And when it would go in the opposite direction, you would get a third and fourth log entry. That's a very simplistic view of it, but what we'll show with the evidence in this case is by doing these type of log entries and this correlation, it's just another way of trying to determine who are the bad guys. Who are the --

THE COURT: Would they have been able to see in the packet?

MR. ANDRE: Yes. So here it does them both on unencrypted and encrypted. But here you can, on the log entry, the key here is just looking at how the packets look and what information you can glean from --

THE COURT: Well, in other words, if you can see it you're not relying on the content, you're relying the format with which the packets are trafficked through the network. Is that accurate?

MR. ANDRE: Absolutely, Your Honor. It is -- the information you're gleaning from thousands of packets coming and going out of network is very telling because you can gather that information and then do a correlation to figure out if these are bad guys who are really clever. I mean, we use very simple analogies here like a mailing label inside of a box because

conceptually that's how they teach it in school, to be candid with you. They use envelopes and they use mailing labels because it's an easy conceptual way to see it. But cyber criminals and state actors who are trying to break into our systems, they can, you know, they can change the address. They have very complex mechanisms to try get in. So these log entries help identify hundreds if not thousands of attributes of these packets that they can look at and correlate and see what is really happening there and try to identify the bad guys.

Now in this case, for this type of packet correlation, this is done in the switches with just the feed back and forth with the StealthWatch. So you have the switches in StealthWatch, and one of the important aspects of StealthWatch is this Cognitive Threat Analytics and the Encrypted Traffic Analytics, because you have to go look at all type of traffic, and you have to be able to do the Cognitive Threat Analytics to do the analysis to determine if there's going to be a correlation of all this information. You need analytics. And so Cognitive Threat Analytics is used for the correlation. The CTA portion of it. And it operates the same way in the routers.

THE COURT: What's ETA? ETA is Encrypted --

MR. ANDRE: Traffic Analytics.

THE COURT: What?

MR. ANDRE: ETA is Encrypted Traffic Analytics.

THE COURT: All right. So it says ETA and then C --

MR. ANDRE: CTA.

THE COURT: Which is what?

MR. ANDRE: Cognitive Threat Analytics. So those two components -- as you can imagine, the Encrypted Traffic Analytics are throughout the entire security system because if -- you can't -- like I said, if you can't read encrypted traffic you're not in business. The Cognitive Threat Analytics in this case are using the correlation data and then doing a correlation, making -- the packet data and doing correlations based on that information.

THE COURT: In other words --

MR. ANDRE: What's that?

THE COURT: The packets that are not encrypted -- I think I asked the same question before -- the packets that are not encrypted, they're stopping the packets based on correlation as opposed to content?

MR. ANDRE: Yeah. It's something that -- when the -- using the correlation technology, it's going to base it -- it's going to stop the package on correlation. It can do it both with encrypted packets and the unencrypted, but it's using the unencrypted portion of the encrypted packets. So the correlation is, it's just another tool in the tool box to try and find the bad guys.

So you have the rule sets, you have the enforcement policies, you have the rapid rule swapping of them, you have the

Encrypted Traffic Analytics, and now you're looking at correlation. This is just that layers of defense.

If you look at Cisco's products and how their data sheets describe the Cognitive Threat Analytics, this is that brain that's within StealthWatch, it says, the very first one it is "The Cognitive Threat Analytics analyzes traffic generated by each user and device. It correlates the data with the organization's broader context to find anomalous traffic associated with command and control -- or command and control communications." That is telling you they're doing the correlation to try to find this, these, this traffic to try to figure out if someone is trying to get sensitive information from you. And we'll have our expert, Dr. Cole, who will be talking about this technology in detail.

THE COURT: All right.

MR. ANDRE: Those are the five patents we'll be talking about, Your Honor. You'll hear from Dr. Mitzenmacher for the first three and Dr. Cole for the next two.

THE COURT: All right.

MR. ANDRE: We have an interesting case here, because not only does Cisco infringe, but we are alleging they willfully infringe. They do it by copying our technology and betraying a trust that Centripetal had with Cisco. They have a history between the two parties. In June of 2015, Mr. Steven Rogers, founder of the company, met with a senior executive at Cisco who

is Pavan Reddy. And they wanted to get together to see if they could work together.

THE COURT: Well, you were engaged but you never got married, is that right?

MR. ANDRE: Well, we kind of got married in 2016, but we never consummated. We got engaged, for sure. We got real close to marriage. We were kind of left at the altar.

So in 2015, this is six months after we launched our product, Cisco showed interest in our technology. And we, we gave them many demonstrations, many meetings in 2015. I got three of them demonstrated here. They were demonstrations that we provided to them. We gave them non-confidential information, our public information. Kind of what we give to potential customers. See if they were interested. They were interested. They wanted to get more information. So in January of 2016 they proposed signing a non-disclosure agreement. And that's what we did. We signed a non-disclosure agreement so we could have a confidential meeting with Cisco and we could provide them with our confidential proprietary information.

On February 4th, 2016, we gave Centripetal -- Centripetal gave Cisco a presentation over WebEx. That's Cisco's Zoom, as it were. That's their technology. And in that presentation we gave them a lot of information. We talked about our algorithms, our secret sauce. We talked about our patents. We talked about a lot of our very sensitive information. There

were follow-up meetings after that with, once again, senior top executives, and later in February and then again in March.

Then Cisco invited Centripetal to be a technology partner at Cisco Live. That's their big annual conference where they invite certain companies in to be partners. We'll be partners together. During that presentation, Cisco even wrote up a nice article on Centripetal's technology, describing it as very favorable. And then at the end of that year, Cisco was provided Centripetal's more proprietary information and information about the patents. At the end of 2016, Cisco said thanks, but no thanks, we're not interested in your technology.

Six months later, they launched their Network Intuitive, their brand-new networking system. And all this time they were hitting our website as well. If you look at that bottom red bar below, they hit our website 354 times during this visit, or at least a Cisco IP address did. They visited 1,200 pages, over 1,200 pages from our website, of how we do things. And if you look at the hits of the website and what they downloaded, you'll see there are certain periods where they were very active. A Cisco IP address was hitting our website very actively during certain time periods. And if you look and overlay that with our meetings with them and right before their launch -- go do the next slide?

THE COURT: Is there an allegation that Cisco made an acquisition of another company that impacted your infringement

claims?

MR. ANDRE: No, Your Honor. Cisco has stated that they bought a company in 2013 called SourceFire and it was a intrusion prevention system nothing like what we're doing. But they bought a security company in 2013 and they're trying to say that they had that technology previously.

THE COURT: So they're saying that that's where they got the technology that you're saying they copied from you?

MR. ANDRE: Exactly.

THE COURT: What was the name of that company?

MR. ANDRE: SourceFire.

THE COURT: Source what?

MR. ANDRE: SourceFire.

Your Honor, just to go back --

THE COURT: When did they buy SourceFire?

MR. ANDRE: 2013.

Your Honor, I'll skip through these slides, but I do want to talk about --

THE COURT: All right.

MR. ANDRE: So as I noted, as I mentioned we had a confidentiality agreement with Cisco. Go to the next slide, please.

That was signed in January of '16. On February '16, we gave a presentation in which we talked about our speed and scale of our technology and how Centripetal's patented filter

algorithms eliminate the speed and scalability problem. We told them about our patented algorithms. That was demonstrated the next day in a follow-up email from our COO, Jonathan Rogers, in which he said the group seemed to hone in on our filter technology and algorithms. There were also a few questions on our patents. This was a day after the presentation. Cisco showed a lot of interest in the algorithms.

Cisco then, as I said, they published information about our technology after we demonstrated it to them. They wrote an entire article on that.

We then gave them, provided them with a management presentation in 2016. This all under NDA. And it was labeled very sensitive. We gave them the RuleGATE Management Architecture. We actually gave them our architecture under the NDA. We told them about our patents. You're going to see a lot of this evidence as we go through it, Your Honor. But what we're going to prove our case on, the infringement case -- and we'll prove our copying case as well -- but the infringement case we're going to show through confidential technical documents, their public documents and statements, their engineer's testimony, the source code, the financial statements, and expert testimony and testing.

Now, their primary defense to this case, and you heard it a little bit yesterday in the tutorial and you it throughout this case, their defense is they use old stuff. They don't use

the new technology, they use stuff from 2013 and even earlier. 2010. Cisco's been in the router and switch business for years. That's what they have said in this Court multiple occasions. They use old stuff. Evidence will tell you that's not true.

June 20th, 2017, this was the press releases. "Cisco unveils a network of the future that can learn, adapt and evolve."

"Cisco's Network Intuitive: The Next Era of Networking." Chuck Robbins, their CEO, expounded that the networking giant new Network Intuitive, saying the company had to rewrite its entire operating system. Think about that. They had to write the entire operating system to enable its command center and analytics platform, Encrypted Traffic Analytics and programmable switches. It talks about they launched a new era in networking. "The Network Intuitive: Breaking down Cisco's biggest innovation in the past decade." That was in June of 2017.

That same press release talks about the Catalyst switches. That was released in June of '17. It says "The Catalyst switching platform. Cisco introducing a new family of switches built from the ground up for the new realities of the digital era." Built from the ground up for the new reality.

You look at their technical documents. On the bottom left there it says "A new era in intent-based. The old technology was video, voice and data. The new era is security."

Top of the list. And they were successful with it.

You saw the COO talk about it in one of the documents. "The Catalyst 9000 switches are the fastest running product in the history of Cisco."

And you put that in the timeline after our meetings with them and when they launched. You look at the Encrypted Traffic Analytics, very important technology. When did they actually do the specifications, the requirements for Encrypted Traffic Analytics? He says early '17. This is one of their engineers who was responsible for it: "You submitted a requirement document in early '17 and at that point you started developing Encrypted Traffic Analytics." That was a month after we gave them all of our confidential information.

And what did they say about Encrypted Traffic Analytics when they released it? Well, they're going to downplay it. In this case they're going to say Encrypted Traffic Analytics is nothing. It's not important. But what you're doing going to see, this is how they describe it even today: "Cisco's Encrypted Traffic Analytics solves a network challenge -- security challenge previously thought to be unsolvable." They released this in 2017. They solved the unsolvable problem. It says "Encrypted Traffic Analytics uses Cisco's cyber -- Talos Cyber Intelligence to detect known attack signatures even in encrypted traffic helping to ensure that while maintaining privacy" so they can determine, detect threats

in encrypted traffic.

In their technical documents they talk about how "Cisco has introduced an innovative and revolutionary technology, Encrypted Traffic Analytics." These are their words: Innovative and revolutionary. They solved the unsolvable problem. They're going to tell you in this case, not important. Encrypted Traffic Analytics is not important. Does nothing. All their documents going up to 2020, this year, they're still saying the same things about it. They're going to say one thing to the court, their experts are going to say one thing. What they tell their customers, what they tell the public, completely different.

Digital Network Architecture. We are talked about that. The DNA. It was released in August of 2017. They talk about the Digital Network Architecture is the new era of networking. That's what they talk about. They talk about it has ushered in a new area of networking with the announcement of intent-based technologies. This was in August of 2017, how they have put security in the forefront. During the tutorial yesterday they said DNA doesn't involve security. Every document they have on DNA talks about security. They said it was just a management center. All it did was manage things. Not true. You're going to see with their own documents where they say the Digital Network Architecture is there for security.

Your Honor, I'll wrap up very quickly here with the

remedies. The remedies in this case, we want past damages for the two years of infringement they had up to the time of this trial. We've apportioned the revenues to the smallest saleable patent practicing unit. We've applied the royalty rate that we've established for those patents, and we're looking for a minimum royalty payment for past damages of between around 445 million to $557 million.

Now, that seems like a large number, but you saw these switches and routers. They're setting records for Cisco. In this short period, they've had over $16 billion in sales of these infringing technologies.

We also want an accounting and all the other, what we're entitled to, the interest and enhanced damages for willfulness.

Going forward, what we ask for, Your Honor, is injunctive relief. We don't want them infringing our technology. Especially on their firewalls. We have competing technology that we're getting killed on. Our sales were doubling year in, year out. When Cisco launches, that stopped. Now we're competing against one of the largest companies in the world against our own technology. We want an injunctive relief on the firewalls so we can get back into that market.

THE COURT: You say the sales, you said they doubled from '14 to '15 and '15 to '16. What have they done since?

MR. ANDRE: They flat-lined ever since. In fact, in

'17 --

THE COURT: What about their earnings?

MR. ANDRE: Cisco's has gone through the roof. These products have set new records for Cisco. As we saw from their CEO, this is the fastest ramping product in Cisco's history because they took something, security, and put it into the network. That was not done. And you'll see testimony on this from their own engineers. No one was doing this in the network infrastructure until they started doing it. Cisco was the first.

THE COURT: All right.

MR. ANDRE: So Your Honor, we appreciate the Court's time and really appreciate the fact that we'll have a chance to do this through Zoom, and hopefully there will be no glitches. So far so good. But we will be presenting a lot of witnesses, fact witnesses and expert witnesses in this case, and we appreciate the Court's time and attention. And at this point I will turn it over to my friend, Mr. Jameson, for Cisco.

THE COURT: All right. Mr. Jameson, are you going to handle that?

MR. JAMESON: Your Honor, Woody Jameson on behalf of Cisco Systems. May I proceed?

THE COURT: You may.

MR. JAMESON: Well, Your Honor, I've been doing this for a long time, almost 30 years now, and I will say that this

is --

THE COURT: Only 30 years?

MR. JAMESON: Only 30.

You say you can't teach an old dog new tricks, but this is a first for me: An opening statement by video conference. So perhaps we can.

That was a lot to unpack, and I'm going to do my best to try to unpack it and share --

THE COURT: Excuse me just a second. I've got some chart here that's covering up Mr. Jameson.

Okay. I've got you now.

MR. JAMESON: Okay. What I was saying is, I've got a lot to unpack, and needless to say, you've been doing this long enough to know there's two sides to every story, and there's certainly a different side to this one, because I disagree with a lot of what I heard.

I want to respond to a couple of your questions at the outset before I turn to my presentation. You asked Mr. Andre about what a Digital Network Architecture is and he -- I think he misspoke. There's a lot of products in this case and it's easy to get them confused. But Digital Network Architecture, it configures routers and switches in a network. It has absolutely nothing to do with threat intelligence. It does not download threat intelligence into the network. But you asked that question and so I wanted to clear that up.

THE COURT: Well, when you're organizing your switches and routers and firewalls, doesn't that involve determining where you're going to put your security within that network?

MR. JAMESON: The threat intelligence is the -- it's the known potentially malicious actors out there. It's the known viruses out there. And threat intelligence is used by any number of companies as a basis to create rules to deal with packets. Bad packets. And the question that you asked was, what does the Digital Network Architecture do. And the only point I wanted to make, because Mr. Andre suggested that that DNA actually is downloading rules with respect to threat intelligence, and that's just not accurate. What DNA does, it allows --

THE COURT: Well, doesn't it create your firewalls and so forth?

MR. JAMESON: No, Your Honor. What DNA does is it literally allows a network administrator to configure a bunch of routers and switches so that they can communicate with each other or the routers and the switches can communicate with computers on a network. It really is an administrative tool. And so that's why I just wanted to respond to that question.

The other question that you raised at the very end of Mr. Andre's presentation was with respect to Centripetal's doubling of revenue from 2015 to 2016, and all of a sudden Cisco started infringing their patents and their revenue just ceased

to exist. And the facts actually tell a different story.

THE COURT: He said they flat-lined.

MR. JAMESON: He said it flat-lined. Exactly.

Well, it did flat-line in 2017. And in fact, in the year 2017, Centripetal did not make a single sale of its RuleGATE appliance, but they do not accuse Cisco of beginning to infringe until June of 2017. So there's a question. What happened in January, February, March, April, and May where they did not have a single sale? And we'll get into that. But it came across as if they flat-lined because we started infringing, and that's just simply not consistent with the facts.

Then -- and we've now heard it twice, we heard it yesterday in the technology tutorial and we heard it today -- about routers and switches basically recently getting the ability to deal with network security. And I will get into this in our presentation in a minute, Your Honor, but routers and switches have been using rules to filter packets for two decades. Going back to, really started in 1998, but it goes back two decades. And so there is a disconnect on that issue between the parties. Routers and switches didn't start all of a sudden being able to filter packets based on rules in the last two or three years. And I will develop that.

Your Honor, Centripetal's patents arise out of a product called RuleGATE. And RuleGATE was a product that was designed to literally use as many as five million rules to

filter every single packet entering a network if a packet had malicious, a malicious -- or it appeared to be malicious based on the application of rules -- the use of five million rules, analyze every packet coming in to a network, and determine whether you need to drop it packet or not, and you need to do that at line speed. That's the product that they were bringing in to the marketplace. And trying to develop that product, it presented a number of problems to the company. And as they solved those problems, they filed for patents. But that's what led to the patents that are at issue in this case. How do we, how do we apply five million rules at line speed to filter packets before they enter the network?

Against that, there are two categories of products that are -- or two types of products that are really being accused in this case. And one of them is the products that use what Dr. Almeroth taught yesterday as NetFlow records.

THE COURT: What he described as what?

MR. JAMESON: NetFlow records.

THE COURT: All right. Now you're saying that they designed these patents to deal with the very large volume of rules that they had to apply. That's why they designed them?

MR. JAMESON: That is, that is -- it was dealing with those problems that led to their patents.

THE COURT: All right.

MR. JAMESON: Five million rules to every packet in

the network without slowing down transmissions. And that led to some of the patents here.

Now, there are two different kinds of products being accused in this case. There are our products that use the industry standard NetFlow, which are not packets, they are summaries of network traffic that have absolutely nothing to do with the problems that Centripetal was trying to solve.

THE COURT: Well, NetFlow, the NetFlow technique is what we've referred to generally as the after-the-fact.

MR. JAMESON: That is exactly right, Your Honor. And Mr. Andre in his opening tried to perhaps confuse or at least suggest that NetFlow has something to do with forwarding packets for analysis. And that's just not right. NetFlow is a summary of network transmissions that are then used after the fact to determine whether or not there might be malicious activity.

Now, there's a different category, the second category of kind of products that they're going after, and that is what I would call the traditional firewall. The traditional end-line appliance that Dr. Almeroth was teaching yesterday that appears at the edge of the network before packets enter the network. And that's the Adaptive Security Appliance and the Firepower appliance.

THE COURT: But that's at the gatehouse?

MR. JAMESON: That's at the gatehouse. And I'm going goat into that in one second.

Those products have been in the marketplace since 2001, and they have been using 10,000 to 20,000 rules applying those rules to every packet that is transmitted across the network to determine whether or not a packet is malicious, and if it is, drop it. And that's where there is a major disconnect in this case, which is these patents, they are late patents in this space. As a result of that, the claims are really, really long, they are really complicated, and they are directed at very, very specific, narrow improvements arising out of this five million rules to every packet at line speed. Cisco's technology has never adopted the five million rules at line speed. They have been using the 10,000 to 20,000 rules for 20 years, they're still using it today. They think their technology is really good, and as a result of that, it's going to result in a lot of non-infringement arguments.

Now, I've done a lot of talking and I haven't even turned to my PowerPoint yet. But unless there are some questions I'm going to turn to my presentation.

Your Honor, I want to talk a little bit about where Cisco originated, because it's a story that's not dissimilar from Centripetal's, except it goes back with 40 years in time.

Back in the late 70s, two individuals, Sandra Lerner and Leonard Bosack. They met at Stanford. They became professors. They were working at Stanford University. And they were trying to figure out a way, how do we communicate across

our campus? And they were working with others, and they figured out a way to communicate with computers across campus by devising this thing called a router. They invented the router. They couldn't commercialize it at Stanford, they had to go into business in order to do something with this technology. So in 1984 they founded Cisco.

I find this -- I think it's interesting paying homage to where they were located -- Cisco comes from the city name San Francisco. Cisco's logo comes from the Golden Gate Bridge. And anyway, Cisco was founded in 1984. They sold the first router in 1986. Today, Cisco's products make up over, well over half of the backbone of the Internet. Over a half of the routers and switches in the Internet come from Cisco.

I want to talk a little bit about Cisco's development of its technology, it's R&D. Based on what you just heard, it sounds like what we do is we just steal company's technology. It's not true. Cisco has over 25,000 patents worldwide. 16,000-plus U.S. patents. We have over 1,300 in the network security space and we have over 800 U.S. network security patents. Cisco employs over 5,000 electrical engineers, and their R&D budget every year is almost $5 billion.

They also teach a lot of people about technology. They're leaders when it comes to teaching people about technology. And Your Honor, if you look at these books, Cisco has a publication company. And if you look at the dates on

these books, it's an important segue to what this case is all about. The first book on the left, the Cisco IOS Network Security dated 1999? Chapter 15 of that book has an entire chapter on filtering packets using rules at a network gateway. That's over 20 years ago.

Mr. Andre suggested that routers just got integrated security in the last couple of years. In 2005, Cisco Router Firewall Security. It's a 900-page book that talks about this firewall security that's in a router.

The Cisco ASA, the Adaptive Security Appliance that's being accused, year 2010, that's the Second Edition. That's not even the First Edition. Predates Centripetal. But it's an all-in-one firewall intrusion prevention system and a virtual private network.

I just point this out because Cisco has been in this space for a long, long time, and they really have been teaching the world how to do this stuff for a long, long time.

This is an important part of this case. It's Cisco's investments and technology companies. Because what you just heard is that basically Cisco thumbs its nose at startup companies and basically steals their technology. And that's just not true. Cisco invests over 200 to $300 million every year in startup companies. Since the year 2000 they've made over 400 investments. And they support emerging technologies. I mean, it makes sense. Cisco wants to know what's cool and

different that's out there, and we will invest in that company, and who knows where it's going to take the relationship one day?

The other thing that Cisco does is it hosts the world's biggest networking security conference every year. It's called Cisco Live. You heard from Mr. Andre that Centripetal was invited to Cisco Live. The reason why Centripetal was invited to Cisco Live was actually because Centripetal was buying threat intelligence from Cisco. Cisco's got a threat intelligence company called Threat Grid. Centripetal was buying threat intelligence; therefore they were a partner of Cisco. Cisco invites its partners to Cisco Live. And unfortunately, even when you get an invitation, it's not free. You've got to pay. Centripetal paid $20,000 to come to Cisco Live to show off their technology to an audience of over 20,000 people that attend this event. It is a boon for startup companies. You've got 28,000 people at a conference to go show how cool your technology is. So it was a great opportunity for Centripetal to come to that conference.

I talked about investments in startup companies. This is just a sampling of the type of companies they have invested in. The reason I show it to you is I haven't heard of a single one of these. Because these are truly startup companies. Cisco listens to pitches all the time in startup companies. Sometimes somebody has something interesting Cisco sees. Centripetal pitched Cisco in this case. Cisco chose to pass. And I'll get

into that.

Finally, a lot of the technology that's at issue here, you asked a question of Mr. Andre about SourceFire. Cisco acquired SourceFire in 2013. That's where the Firepower appliance comes from that's at issue in this case. Very important point. SourceFire entered into business in 2001 and they've been selling a firewall appliance since 2001. Cisco now owns that company. Why do we own all these different companies and why did we acquire them? And this goes to the point that Dr. Almeroth made yesterday. He talked about defense in depth. That in network security, there's not one cure-all for network security. You have to attack network security from every angle possible. That means stopping threats at the entrance to the network. It means analyzing threats after they have entered in the network, and what can we do to stop it from happening again? Do we need to quarantine a computer? Do we need to shut down an entire set of computers? And that is the defense in depth approach that Dr. Almeroth was talking about yesterday. And these acquisitions, along with Cisco's own innovations, it allows Cisco to sell what I would call a holistic approach to network security. Firewalls at the network gateway, back-end security after the fact, to figure out how to remediate something that's already gone wrong. So it's a holistic approach that Cisco takes by way of its product offerings.

Now I want to turn to the technology that's at issue

in this case. And a quick refresh just to orient you, Dr. Almeroth talked about the end-line appliances yesterday and the out-of-band NetFlow based appliances. Two different approaches to securing an area. You remember this, this is the guardhouse approach. Every packet is analyzed. Again, I show here 10,000 rules being applied to every packet to determine whether something is malicious, drop the packet if it's malicious. Your Honor, the title here, SourceFire Pioneered Guardhouse Approach in 2001. SourceFire is now owned by Cisco. Cisco bought SourceFire in 2013. What I'm showing on this slide here has been in the marketplace for almost two decades now. You remember the pros and the cons. Guardhouse approach. False positives. Possible bottlenecks. Latency. Added delays. It can be expensive depending upon how many entrances to the network you have, and then the most upside and the downside of automation.

Very important, Your Honor. This is Centripetal's RuleGATE. This was the appliance that Centripetal was developing that led to their patents. It is an appliance that sits at the edge of the network. We call it a -- well, we don't. Witnesses call it a huge guardhouse on steroids. Because it's not using 10 to 20,000 rules, it's using five million rules to every single packet without slowing down network traffic. I can't comprehend that. But that was what they were trying to take to market.

The downside of RuleGATE is the same. It is really the same downside as using 10 to 20,000 rules but it's magnified. Potentially more false positives, more added delays, it's going to be expensive because of the processing that you need, and both the pros and the cons of automation.

Now, you heard about all the presentations made to Cisco by Centripetal which led to us stealing their technology, according to Centripetal. What I'm showing you here, Your Honor, this is a presentation that was made by a company called Oppenheimer to Cisco. Oppenheimer was retained by Centripetal to go into the marketplace to try to raise capital for Centripetal. Oppenheimer made this presentation to Cisco at the end of 2016. Oppenheimer's work with Centripetal, it was called Project Cedar. That was the code name for Centripetal, Project Cedar. And this is how Centripetal's technology was described to Cisco. "The fence must be done in real-time while the traffic is passing. Unless each packet is examined in-line, it isn't possible to get a true Prevent posture with intelligence. Looking at network traffic and data in-line is extremely challenging. The biggest hurdles are scale and latency." Again, the bottlenecking issue and how are we going to deal with all these packets using five million rules.

And then here is what's really important. This is how the patents were described. "Project Cedar has been awarded patents for its computational processing algorithms that allow

the threat intelligence to be applied in-line in real-time without network traffic latency. Additionally, the company also has a comprehensive system of patents around threat intelligence gateways. The threat intelligence gateways.

And Your Honor, the patents awarded for computational processing algorithms? Sidenote: Those patents are not being asserted in this case. Those patents actually, they bought those patents as part of an acquisition from a company called Great Wall. They didn't invent that, they bought it. And those are not being asserted in this case.

So RuleGATE and Centripetal are about patents at the threat intelligence gateway. Where is the threat intelligence gateway? Your Honor, it's right here. It's at the edge of the gateway to the network, where we're going to protect, we're going to protect the network from all these packets getting in that are potentially malicious. That's what their patents were dealing with.

Mr. Andre said that we led them on for a couple years and then we finally took a pass in 2017 after we stole their technology. That's not entirely accurate. The first pitch that they made to us was in February of 2016. And that was actually not Oppenheimer, this was Centripetal when they made their first pitch to us. And they made a PowerPoint presentation. Following that presentation, the people from Cisco that listened to that presentation, they had internal email feedback. And

here is what they said. I'm going start right here. "Centripetal is an Internet prevention system on steroids" -- excuse me. "Intrusion". I keep on getting that wrong. "Centripetal is an intrusion prevention system on steroids. Meaning they have larger signature base than we did at SourceFire, approximately 10,000 rules, having their five million rules in 10 microseconds." And let me ask you a question. Why does it say that we did at SourceFire? Because the people that were receiving this pitch were former SourceFire employees that, when Cisco bought SourceFire in 2013, they became Cisco employees. So they're comparing what Centripetal is doing today or what they're saying they can do with what SourceFire was doing in using 10,000 rules.

Then we go on and I have it highlighted in yellow, "We also went through this at SourceFire and it created its own set of risks for us in terms of supplier viability, cost effectiveness, et cetera. Another way to quote Steve Jobs would be to say unless there is an order of magnitude improvement in performance, 10X, the status quo is good enough."

Cisco made the internal decision, what we're doing, 10,000 to 20,000 rules and we've been doing for almost two decades, it's good enough. We don't need five million rules and the problems that are going to be associated with that.

Ten days later, internal correspondence at Cisco. And Your Honor, in this email these are individuals that

participated in that meeting. Karthik Subramanian, who will be a witness in this case, and he sends an email to Prasad Parthasarathi. Background on Centripetal. He asked a question. "What is the consensus view on this, question mark. I think it's a pass, given feedback on everything else. Agree, question mark?"

Mr. Parthasarathi responds, "Yup, agree."

Mr. Parthasarathi then called Centripetal, Mr. Jonathan Rogers, and said to Mr. Rogers in February of 2016, "We're not interested in investing right now."

Then we fast-forward. Later, 2016, this is an Oppenheimer document and it shows that Oppenheimer, he reached out to 148 companies in the marketplace trying to get someone to invest capital in Centripetal. And with respect to Cisco, they approached us late 2016, it was November 8th, 2016, they sent a teaser on November 15th. They have the entry, Cisco passed. They then have another entry, they actually followed up with us on January 6th of 2017, and Cisco responded they will reach out if there is interest. Cisco said again, thanks, but no thanks, we're not interested in investing in Centripetal.

So they make those pitches. It's about the in-line appliance. We're not interested. But this lawsuit's not about purely in-line appliances. It's quite frankly about every network security offering that Cisco has.

I want to now turn to the after-the-fact system as

you've now dubbed it, that will allow and detect out-of-band system, and you will recall from Dr. Almeroth yesterday that the out-of-band system based on NetFlow is where summaries of communications are put together and sent to a flow collector by routers and switches. Packets aren't forwarded. It's a summary of communications. And so much NetFlow technology is being accused in this case that it's important to note that Cisco invented NetFlow in 1996. Over 25 years ago. And NetFlow became an industry standard in 2004. It was standardized by the Engineering Task force, the Internet Engineering Task Force. And Your Honor, there are five patents being asserted in this case. You can read the specifications from start to finish, you can look at the asserted claims, and the word NetFlow and industry standard that's been around for 15 years doesn't appear in any single patent. StealthWatch, Cisco's product, it was acquired from Lancope. It's one of the accused products. Dr. Almeroth took you through this and -- let me -- I'm sorry, let me back up.

Again, StealthWatch, it's just, it's consistent with what Dr. Almeroth showed you yesterday. NetFlow records are sent to StealthWatch, StealthWatch analyzes those NetFlow records, if they think that there's something malicious in the network, StealthWatch can then send an alert to an IT manager to decide whether to take action. So that's what NetFlow and the Allow and Detect system is about.

Okay. Here are the products at issue. There's eight different products. There's accompanying software that they're accusing. Catalyst switches, Aggregation Service Routers, Integrated Service Routers, Cisco's bread and butter. I give you the dates here just as point of reference. They're obviously not accusing -- by definition they're accusing successor products to this -- but it's just to give you an idea of how long these products with have been in the marketplace. And so that's a reference point for you.

This is where things get really complicated. Hopefully this is a cheat sheet for you. But with respect to how they're accusing us of infringement, these are all of the various combinations. And it is the proverbial kitchen sink. I have in the pink box, or whatever this is, whatever color that is -- I highlight, I highlight the ASA, the Adaptive Security Appliance in two places because the ASA, which includes the Adaptive Security Appliance and the Firepower appliance, those are the only two appliances that are firewalls that are located as an entry point to the network to analyze packets based on packet filtering rules, all the other combinations are dealing with ethernet flow or out-of-band configurations.

Now, Dr. Almeroth taught this yesterday. This is with respect to the accused in-line Adaptive Security Appliance and the Firepower appliances. They're right here in the network. The Firepower Management Center, it can interact with that

appliance. And those appliances don't infringe. And in a nutshell, here's why.

The two patents that are being asserted, again, they arise from the problems associated with using five million rules to filter packets at line speed. These appliances continue to use the same technology -- and don't get me wrong: These appliances have new technology in them. Well, of course they do. They get updated with software updates and things like that. But with respect to what they're accusing, they have been doing this stuff for 20 years.

And here is the issue for Centripetal: They've got to figure out a way to walk the infringement invalidity tightrope. And here is what you're going to see, Your Honor. When we get into these claims of the '806 and '205 patent, they're really long, they're really complicated, and they're really specific. And the reason for that is, is because they're trying to get a patent in an area that is so well developed that it's got to be really, really narrow. It's got to be a narrow improvement. And it's that narrow improvement that we have not implemented in our technology. And so in order to prove infringement, they gloss over the specification and they talk in big-picture generalities. And they'll talk about these appliances have, they have rules, they filter packets, they drop packets and things like that. But if you can choose a word here from a marketing document and another word here in another marketing

document and you can put together an infringement case that way, well, we can go back in time and do the exact same thing. And it will prove that the patents are invalid. So that's the tightrope that they're on.

Now, with respect to the other set of products, and this is the products based on NetFlow. And I'm going to get to the end of this for sake of time and then try to orient you.

Okay. Right here. Just to orient you, the routers and the switches, they can send NetFlow to StealthWatch. StealthWatch can analyze that NetFlow, and if they think something's up, they can send an alert to a system administrator. That's one way to send an alert to a system administrator.

The next way, StealthWatch can send the NetFlow on to Cognitive Threat Analytics. CTA can do an analysis. And if they believe that something's suspicious, CTA can send and alert back to StealthWatch, and then StealthWatch can send an alert to the system administrator.

In yet another way, is with what's called Encrypted Traffic Analytics data. It's two additional fields that were added to NetFlow, and we'll get into that. And using NetFlow with ETA, again, the NetFlow record can be sent from StealthWatch up to the CTA, you can analyze it, if there is something up, you send the alert back to StealthWatch and then on to the network administrator. And then that network

administrator has that little whatever that is, that halo or -- not halo, but whatever it is above his head. At that point, the network administrator has to make a decision. I've got possibly malicious activity in my network, what do I do? If he wants to take action, send a message to the Identity Services Engine, IT manager who is handing the Identity Services Engine, we've got a problem in our network, we need to shut something down. The identity Services Engine will communicate with the router or switch, and we're going to shut off User Computer No. 2 because something is up with that computer. And every bit of these scenarios, every bit of this is based on NetFlow records. And the allegations against NetFlow, they fail. And that comes right out of multiple witnesses from Centripetal you're going to hear from in this case. Centripetal does not use NetFlow. The founder of the company, the inventor of '205 and '806 patents, we asked him, "To your knowledge has Centripetal ever done any development work in developing a security product that's based on NetFlow?

"Answer: No. It's a different market."

Asked him again: "Did Centripetal do any development work to develop a product based on NetFlow and the application of threat intelligence?

"Answer: I already told you we did not do anything with NetFlow." He disparages it. "It's not really good for cyber protection."

So we asked the chief technology officer of the company, Sean Moore, "So, did Centripetal have any technology solution in its product lines for looking at NetFlow records, analyzing then and raising alarms or not, based on NetFlow?

"Answer: I don't believe so."

We didn't stop. We asked Mr. Rogers' son, Justin Rogers, the principle engineer, "Question: Centripetal's technology did not analyze NetFlow; is that correct?

"Answer. No, it did not."

Back to my point, the words NetFlow will not appear, do not appear in any patent being asserted in this case.

Now we fast-forward to 2000... Your Honor, we now fast-forward to 2019. And this is from Chris Gibbs, he's the vice-president of sales at Centripetal. He's actually a former Cisco employee that Centripetal hired away. And here's what he said to customers comparing Centripetal's products with Cisco's. And this is, by the way, this is July 22nd, 2019. We've already been sued, okay? We've been sued, and here's what he says:

"AMP, Advanced Malware Protection, is a capability that is bundled into the Cisco Adaptive Security Appliance with Firepower services firewall. Most importantly, AMP is looking at malicious files that have entered the network. This is a classic allow-and-detect scenario. Centripetal's solution is different. We block at the network perimeter. Two different types of tools."

We don't infringe based on anything with NetFlow.

So, your Honor, why are we here? Well, one of the reasons why we're here is because, unfortunately -- and this is with the benefit of hindsight -- unfortunately we chose not to invest in the company. And what I'm showing you here is, on the left-hand side, these are not Centripetal employees, these are representatives of Centripetal. These are the typical people that are in the investment industry that are trying to make connections for purposes of doing a deal. And between May of 2015 and October of 2017, all these individuals on the left made a connection with somebody at Centripetal with these various Cisco employees. So we were being contacted on a fairly regular basis, multiple different entry points into the company for the better part of two years. And they're asking us, invest in the company. So why do we visit their website? Well, they want our money. We want to know what they're doing. So a lot of these people are visiting this website, and it's coming in multiple entry points. We chose not to invest.

Now, Your Honor, Encrypted Traffic Analytics, it came into the marketplace in June, 2017. They basically say we stole Encrypted Traffic Analytics. This is internal email correspondence within Centripetal, January 15, 2018. This begins with Jonathan Rogers, he is the current chief operating officer, and he thought Encrypted Traffic Analytics was based on Centripetal's meetings with Cisco. And here is what he said.

And I've got the timing down because this happens over the course of four and a half hours. He says to his dad and to Sean Moore, the chief technology officer, "I hope you guys are sitting down when you watch this. I knew it was flagrant, but not this flagrant. Has this moved to the top of the list?" Apparently at this point they're looking at whether or not they want to monetize their patents. Has it moved to the top of the list. Immediate response from Sean Moore, literally 15 minutes later. "I don't think there is direct infringement here. They're using artificial intelligence, machine learning to detect off-line. Basically their technology solves a different problem altogether." And he says "We looked at this about six months ago and determined it was not an infringement then."

So Mr. Moore immediately is saying I already looked at this before, ETA, that's not infringing technology.

But here's what happens. His boss follows up and says "It looks like they're doing exactly what we have patent and say so in a white paper."

And then the owner of the company follows up seven minutes later. Literally seven minutes later. "I agree. It looks like a pretty clear case of infringement."

Sean Moore, 2:36 in the afternoon, literally in four and a half hours, "I reviewed the data sheet, white paper that Jonathan attached. Yes, there are many infringements in several of our patents, patents families." So literally in four and a

half hours on one day, Centripetal has decided that Cisco's technology infringes a bunch of patents.

Now, here are the facts about Encrypted Traffic Analytics. Mr. Andre told you in his opening that we started developing Encrypted Traffic Analytics in 2017. It's not true. We started development work by an individual named David McGrew who is going to testify in this case, and we started that development work in 2015. Mr. McGrew actually filed for a patent on it August 6th, 2015, and it's now issued as a U.S. patent. He began publishing his research to the industry in January of 2016, and he was publishing his research and it was peer-reviewed at academic conferences throughout 2016. And he will testify under oath he had never heard of Centripetal until the middle of 2017. ETA development work began in 2015. This is before Centripetal had even filed for patent protection on the '806 patent that they're claiming is infringed by Encrypted Traffic Analytics.

So the final reason why we're here. Centripetal's been in business for 10 years now. As of 2019, their total product sales were $9 million. They have had as many as 55 employees. $9 million over 10 years with 55 employees does not work. They need alternative sources of revenue, and therefore, you go after the biggest network security company in the country.

Okay. I want to briefly hit on copying and try to

wrap this up. Your Honor, we've been asking in discovery and we're going to be asking of every witness, what is it that we stole? What is it that we copied? They won't tell us. They tell us, ah, you stole our patented technology. Ah, you stole our innovations. But what is it on this list that we actually stole? What is it that we incorporated into a product that we took from you? They won't tell us, because we didn't take anything. And they're not going to have a shred of evidence on that.

I know -- Your Honor, can I have five more minutes? I know I'm at the limits.

THE COURT: All right.

MR. JAMESON: Thank you. Okay.

Zero evidence on copying. And we asked a number of witnesses about copying during the case, and these are the types of answers that we got.

"Did you ever tell Cisco any confidential information?"

"Answer: Not to my knowledge." Says it again.

Chris Gibbs, who went to Cisco Live, same question, "Did you disclose any confidential information to Cisco?

"Answer: I would never do that."

We talked about the website visits. Every Centripetal witness has confirmed there's no confidential information on their website. In fact, it doesn't make sense. You don't put

confidential information on a website. Their copying story doesn't add up. We invest in startups all the time. 400 times over the last 20 years. 200 to $300 million a year. Centripetal is trying to raise $20 million. If their technology was interesting, we would have invested.

We could flip the script though. If there was true evidence of copying, this is the type of thing you might see going the other way. Centripetal, they hired our employees. "Preference for Cisco and SourceFire security experience." We didn't hire any of their employees.

Okay. When it came time for them to develop the RuleGATE product, called the Cisco Graphical User Interface, which is this screen right here on a monitor, the person developing that, the person developing that at Centripetal, he admitted in his deposition that he looked at Cisco's graphical user interface and he used that to develop RuleGATE's graphical user interface.

We asked Doug DiSabello about using SourceFire, which is now Cisco, certain design documents. And we asked him, why are you referencing design documents in internal emails? And the answer is, well -- the question was "So for designing Centripetal's next RuleGATE product, did you look at other people's websites including Cisco's?" And the answer was, "I believe so." And it was a reference to this. Let's use Cisco's design documents.

Another example. This is from the founder of the company. "There was some publication about a Cisco OpenSOC technology." I'm at the bottom here. "From Pierre Mallet to Steve Rogers. "If they can do it, then so can we."

Steve Rogers to Justin Rogers: "Should we download it and check it out?"

That's what people do with Cisco's technology. But it wasn't going in the other direction.

When it even came to marketing materials, this is a Centripetal document. This is not a Cisco document, this is a Centripetal document as an example of what good marketing is. And we asked Justin Rogers, "And why did you choose to use Cisco as an example as opposed to any of the other companies in the cybersecurity space?

"Answer: Because they're the No. 1 IT company. Why wouldn't you want to borrow from the best IT company in the world?"

And then finally on copying, this is from Haig Colter, another Cisco employees -- excuse me, a Centripetal employee they hired away from Cisco. "Subject: Support ideas to copy." And he attaches a SourceFire customer data sheet -- again, SourceFire is Cisco -- and these are ideas to copy. We were a resource for them as they were trying to get off the ground.

So what do you do? You sue the biggest company in the network security space, you assert 11 patents, we're only

litigating five today, you accuse our entire product line, you tell a bad-actor story, and you hope for the 545 million dollars that Mr. Andre said that they were seeking in damages.

And so with that, Your Honor, this is in response to our 250-page findings of fact and conclusions of law. What we've tried to do here is, for each patent, we give it a short-form name. We give it a short summary as to what we think the patent is about. We give you a thumbnail -- and these aren't all our non-infringement defenses, be crystal clear, these aren't all of them -- but here is a thumbnail as to why we don't infringe, and then these are the claim elements, primary claim elements that we are going to be focused on in this case. And it's not all of them. Because a lot of what we focus on is really going to depend on what their experts say. But we think this is where the case is going to go. And we've done this for every patent -- and Joe, can we go to Slide 82 and I'll wrap up.

THE COURT: Well, your time is about up.

MR. JAMESON: Okay. This is my last slide.

And this is invalidity. Your Honor, this is the infringement goose and the invalidity gander. And what's good for the goose is good for the gander. If they're going to piece together from marketing documents here and a marketing document there, a word here and a word there, and these words appear in this claim and therefore Cisco, you infringe, well, we're going to go back into our predecessor products and our predecessor

documents and we can do the same thing. And so that's what I mean by the goose and gander rule on invalidity. And Your Honor, that's the appropriate measure of damages in this case, zero dollars.

And I appreciate you putting up with me during this opening, but thank you, and we look forward to trying this case.

THE COURT: All right. We'll take a recess and resume at 12:20.

(Recess taken from 12:05 p.m. to 12:23 p.m.)

THE COURT: All right. Is the plaintiff ready with his first witness?

MR. ANDRE: We are, Your Honor. This is Paul Andre for plaintiff Centripetal.

THE COURT: All right.

MR. ANDRE: At this time we are going to have Mr. Steven Rogers to turn on his video and his audio.

THE COURT: All right.

MR. ANDRE: I see him on the screen now, so I think we're ready to proceed, Your Honor.

THE COURT: All right. You may proceed.

STEVEN ROGERS, having been duly sworn, was examined and testified as follows:

MR. ANDRE: May I proceed, Your Honor?

THE COURT: You may.

MR. ANDRE: Thank you.

DIRECT EXAMINATION

BY MR. ANDRE:

Q. Good afternoon, Mr. Rogers.

A. Good afternoon.

Q. Would you tell us where are you currently work?

A. I work at Centripetal Networks.

Q. And what is your title?

A. I'm the founder and CEO.

Q. Before I talk about Centripetal, I want to talk a little bit about your background.

THE COURT: All right. Ask Mr. Rogers if he can talk just a little bit louder?

MR. ANDRE: Sure.

Mr. Rogers, do you have a microphone handy?

THE WITNESS: Yeah, let me see. Let me see if I can adjust here. Hold on a second and we'll see if there's anything that can be done.

MR. ANDRE: If you speak up I think that's all you can do at this point.

THE WITNESS: Okay. I set the volume up a little bit. All right. Is that better?

THE COURT: Yes.

THE WITNESS: Okay. There we go.

MR. ANDRE: Thank you, Mr. Rogers.

BY MR. ANDRE:

Q. Let's start with your background. Where did you go to college?
A. I went to Virginia Tech.
Q. And when did you graduate?
A. I graduated in 1974.
Q. And what degree did you get?
A. Electrical engineering degree.
Q. And what did you do after you left Virginia Tech?
A. Well, I was in the Corps Cadets as a ROTC student, so I did the normal thing, which was to go into the military.
Q. Which branch?
A. The Air Force.
Q. And what type of work were you doing at the Air Force?
A. Well, I worked in an organization called the Air Force Security Service, it's --
Q. What is it?
A. Yeah, it's not what you think. It's not like the Security Police. But the Air Force Security Services is that part of the Air Force that connects in to NSA, and its mission is to help gather intelligence, particularly in wartime situations, and also to protect U.S. assets against threat and exploitation.
Q. What type of assignments were you given as part of the Air Force Security Services?
A. I had a number of really interesting and exciting, for me, assignments. Are assignments I was responsible for security on

the AWACS, which is this big airplane that has a huge radar dome on the back of it and can fly near a battle zone and control all of the battle, all the airplanes and everything, all the fighters involved.

I also was responsible for Air Force One almost my whole time in the Air Force, my whole five years.

And another project I did was the securing of the National Military Command Center, which is built in the Pentagon. That was a newly constructed center, and I was sent with a team to assure it for security.

Q. And were all these projects related to making sure the communications between Air Force One and who it was communicating with and the AWACS secure communications?

A. Yes. And space-based, you know. Air-based. Land-based. All kinds of different systems that we had.

Q. And at this time, back when you were at Virginia Tech or in the Air Force, did you do any kind of work with cybersecurity?

A. Well, cybersecurity didn't emerge until the early 2000s as an issue that we would really be concerned with. So, but what I dealt with was the precursors to all of that. The idea of securing communications and maintaining its security through a variety of means.

Q. And when you were at the Air Force did you get any kind of awards or medals or commendations?

A. Yes. Actually for the AWACS program I received an Air

Force Commendation Medal. For the National Military Command Center I received a second Air Force Commendation Medal. Then for one project that was particularly important, space-based system, I received a Defense Meritorious Service Medal, which is pretty unusual for a First Lieutenant.

Q. Now, after you left the Air Force you went to work with the Sperry Corporation. What kind of company is that?

A. Sperry is a defense contractor, what we would call a systems integrator. They built systems for defense purposes.

Q. And what did you do for them?

A. Well, they hired me to be the architect of a new system they were building that was designed to train intelligence-gathering people in a wartime scenario. So what this system had to do was to replicate all of the signals traffic, all of the types of intelligence there were during a wartime scenario, all in sequence, and would allow people to use equipment that was the same that they would use in real life to be able to gather intelligence and counter threats. Naturally you don't want to have to learn these skills in an actual war environment. Ahead of time. So that's what the system had to do. It was quite complex.

Q. And what did you do for the Harris Corporation?

A. Well, when I was at Sperry, the NSA determined that they needed to develop countermeasures for a problem that I discovered. Remember I mentioned the Defense Meritorious

Service Medal project. So they came and asked me to consult for them through Harris Corporation. And because of the significance of that effort, I really needed to do that. So I left the Sperry organization after I completed the development of the architecture and then went over to Harris, and worked on that program for three years.

Q. And next on the list is a Cryptek Secure Communication. What was that company about?

A. Well, while I was in the Air Force, you know, I saw what the secure communications environment was like and decided that we needed to have a new type of secure coms terminal. So at the time the military had secure voice terminals, but they had no good way of transmitting graphics information. So what we decided to do, what I decided to do is to found a company that would build a secure fax machine. And at the time that was, you know, really great technology. And we built that machine from the ground up. All in the United States. It was the only all-U.S.-made such machine. And it had the ability to be encrypted in its traffic and secure in many other ways that you couldn't get from a standard device. And that machine was very successful. It sold all over the world. It became the standard for the U.S. Navy, Army, Air Force, for the White House Communications Agency. Traveled with the President. Traveled on Air Force One, of course, which I was familiar with that environment. And it was a quite-successful product for many

years.
Q. I see there's a Cetacean Networks. What was that company?
A. Well, Cetacean Networks was in some ways an outgrowth of the Cryptek. So the next thing beyond static graphics is real-time traffic. And at the time, the Internet was coming into its own, and so the thing about the Internet is that it's asynchronous; that you send packets of data on the Internet, they don't necessarily arrive all on time. So what we did was we designed and built a router system that would provide the Internet with the capability to have lossless delivery over the Internet and the absolute fastest delivery of every packet. So it meant that your voice and video didn't have to be delayed or disrupted or interrupted in any way at any time.
Q. The last one before we get to Centripetal is Rivulet. What was that?
A. Rivulet was a follow-on for Cetacean in a way. And what we wanted to do was develop a complimentary system that would run on Local Area Networks that would provide the same quality, but it didn't require you to put in a new switch or a new router.
Q. And that brings us to Centripetal Networks. When did you found Centripetal?
A. I founded it in 2009.
Q. Now, if we look at your background here from the time you went to Virginia Tech in 1970 until today, approximately 50 years, has most of your work been involved with some type of

security or secure communications?
A. Well, I have done both communications and security in my career, and the two combined together.
Q. And how is the 50 years experience over that time that you founded Centripetal 40 years of experience, how did that influence your thinking as to what type of company Centripetal was going to be?
A. Well, I saw the Internet, the Internet of course was a direct line outgrowth of messaging systems pioneered by the military that I tested while I was in the Air Force. So I saw the development of that, realized what the security problems were likely to be, saw the growth of cybersecurity issues, and decided that we needed to have a fresh look and a new type of solution that would be much, much more effective than what we had in the early 2000s.
MR. ANDRE: We can take that slide down.
BY MR. ANDRE:
Q. Now, first of all, the name Centripetal, how did you come up with the name?
A. Well, one way to think about the Internet is that it's a, it has a tremendous benefit in that anyone can communicate with anyone anywhere on earth. And that's a hugely powerful thing. The bad part about it is that anyone can steal from anyone anywhere on earth. And you can cross legal jurisdictions when you steal. So a criminal in one jurisdiction can steal from

somebody in another jurisdiction and it may not be viewed as criminal in his original jurisdiction. So that's a really bad thing. And it allows crimes to multiply. So that was very concerning to me. And what I wanted to do was to come at it with a solution to give control over who comes into your network back to the user, instead of just hooking up to the Internet and having all sorts of criminals come in to your network.

Q. What was your understanding of how cybersecurity was being handled in 2009 when you formed Centripetal?

A. Well started out as a, I think if I could characterize it simply, it was a -- the idea of cybersecurity was to look at the "what". So when a criminal or anyone would send something to you, let's take a look at that and see what it is and see if it could be bad or not. And the problem with that idea of "what", as it turns out, there's an infinite amount of "what" that's bad that a criminal can send you. It just infinite. And so these systems for looking at "what" started to work, but then they started to fall apart and not defend appropriately, because all the attacker had to do was just make a little change to the "what", a tiny change, and it wasn't detected anymore, so it wasn't stopped. And so cyber attacks increased exponentially.

Forgive me for the long-winded answer here.

So our idea, which is quite different, but one that came from my experience in the intelligence community, is let's use intelligence instead to decide what comes in your network.

Let's take the knowledge of who's bad, okay, and use that to stop what's coming.

Now, people may say, well, there's a lot of bad guys out there so that's a pretty big problem. It is a big problem. But the thing of it is, is it's not an infinite problem. The "what", that's an infinite problem. You're never going to solve the problem that way. And we haven't. But the "what", that's a big problem, but it's a solvable problem. It's --

Q. The who?

A. -- hypothetically solvable. So that's what we did.

Sorry for the long explanation.

Q. Let me show you what's been marked for identification as PTX240. Do you know what this document is, Mr. Rogers?

A. Yes, of course.

MR. ANDRE: Go to the cover page, please.

BY MR. ANDRE:

Q. What is this document?

A. Well, it's a white paper to help people understand why what they're doing isn't working.

MR. ANDRE: Your Honor, I'd like to admit into evidence PTX240.

THE COURT: All right. PTX240 will be admitted.

(Plaintiff Exhibit PTX240 received in evidence.)

BY MR. ANDRE:

MR. ANDRE: If we go to the first page of that document right after the cover page, Your Honor. This should be in the witness binder.

THE COURT: It is.

BY MR. ANDRE:

Q. The second paragraph on the left-hand column talks about some of the problems with the Internet growth. Could you describe how this informed your understanding of what the market looked like in 2009?

A. Well, sure. So what was happening by 2009, we had about 10 years of Internet. We started to have quite a few attacks, large cyber breaches, that kind of thing. So it was emerging as a problem. So at the same time the Internet was showing a great deal of promise. So that meant that the network was stretching and reaching every single house, business around the world. Every government agency and so on. So it was displacing other networks. And so that presented a problem for the Department of Defense, because it found itself needing to use the Internet in the conduct of its business. And so they ended up forming the Cyber Command to deal with this problem because it had reached such a, such an extent.

Q. If we go on that same page on the right-hand column, there's a description of Internet cyber attacks and conventional defenses. Do you see that?

A. Yes.

Q. Could you describe the types of attacks you were seeing at that time period?

A. Well, there are two general types of attack, and that's still true today. There's the idea of denying service. That's a rather, you know, brute-force type of attack. But it's where you send data in packets which can come from anywhere to somebody's network device or network connection, and you flood that thing with so much data that the person or the entity, the company, can't use the Internet anymore because there's so much data coming. And so that's one type of attack.

The other type of attack is one where you try to steal information. And at the time this was written, the main way you would do that is to implant some malware of some kind inside the end-user's device, and that malware is basically just a program that will look around inside your computer and send out stuff that you don't want sent out. You know, send out your private information to the attacker.

Q. Thank you. Let me show you another white paper that was written around the same time, and this is Centripetal's solution to these problems, PTX1591.

Mr. Rogers, do you know what this document is?

THE COURT: PTX1591. All right.

MR. ANDRE: Yes. Your Honor, I'd like to move PTX1591 into evidence.

THE COURT: PTX1591 will be admitted.

(Plaintiff Exhibit PTX1591 received in evidence.)

BY MR. ANDRE:

Q. Mr. Rogers, what was the purpose of writing this white paper?

A. Well, the two papers kind of go together. One paper explains why things aren't working, and the other paper explains what you could do to solve the problem. It's pretty much as I described it before: What you need to do is start using intelligence to guide your defense instead of trying to just look for "what". And so we developed a system called RuleGATE, and the network protection system and all the technologies to go around it, because if you're going to apply intelligence, it's quite a difficult technology to build to have that intelligence then effectively protect your network.

Q. If we go to the second page of this document there's a summary, and the first sentence of that summary states that "Conventional cyber defenses - network, firewalls, routers, web proxies and intrusion preventions systems, IPS, are rapidly losing effectiveness as the size, power and dynamics of the cyber threat increase at a prodigious rate." What do you mean when you say that the firewalls, routers and web proxies are losing their effectiveness?

A. Well, I can give many examples, but it relates back to what I said about the "what". So for instance, a firewall, very

static device. Has a very small number of things that it can look for in terms of "what". And it basically failed. It failed in security. That's why we have all these breaches. Every one of the major companies and government organizations that was breached in that era, they had the firewall. They probably bought the firewall from the, you know, the best vendors. The IPS is an example of a "what". So what it does is it looks at a file that comes in your network and says what signature does this have, a signature being a calculation of what is the code in there.

When they started out, these IPS devices would have the ability to look for some thousands of signatures. But what the bad guys found out is they could expand that to hundreds of millions of signatures, and so the percentage of things that you could actually find just went down to zero. In fact, the bad guys found that they could put a new signature out for every single attack so that there was no way you could have the prior knowledge of the signature of their particular attack. So these things failed and left the industry with a growing cyber problem that was basically growing exponentially.

Q. And the next sentence says "Today there exists asymmetry between cyber defense and cyber threats. "What does that mean, asymmetry between defense and threats?

A. Well, the way asymmetry comes about, because the attackers are able at very low cost to mount a very big and complex

attack. The defenders can't do that. They don't have enough. They can't put enough investigations of "what" at this time up against the attackers. So they don't have a way, really, to defend against it. So it creates a asymmetric situation. It's a thing you don't want in certainly any military environment. You don't want, you know, a small band of people to be able to take down a whole battalion of Marines. That wouldn't be very good.

Q. Now, how did Centripetal's technology try to change this asymmetry between the cyber defense and cyber threats?

A. Well we, as I mentioned earlier, what we did was we want to transform the problem so that the solution -- a different solution could be applied. That solution is to use threat intelligence to identify the "who".

Q. Let me show you what's been marked as PTX231.

Mr. Rogers, do you recognize this document?

A. I do.

Q. What is this document?

A. Well, this document goes beyond the last two, and the idea is to help explain to people who are charged with defending their network, why they would want to go to an intelligence-based defense.

MR. ANDRE: Your Honor, I'd like to move Exhibit PTX231 into evidence.

THE COURT: All right. PTX231, I noticed the other

exhibits had a date on them. I'm looking at the first couple of pages. I don't see dates. Do we know when this was published?

MR. ANDRE: It looks like May of 2018 is on the last page, Your Honor. Well, maybe 2019. Copyright 2019.

THE COURT: Says Copyright 2019.

MR. ANDRE: Yeah.

THE COURT: All right. Okay. PTX231 will be admitted.

(Plaintiff Exhibit PTX231 received in evidence.)

MR. ANDRE: Thank Your Honor.

BY MR. ANDRE:

Q. Mr. Rogers, the title of this is "Far Beyond the Firewall: Centripetal's CleanINTERNET Service." What is CleanINTERNET?

A. Well, what we discovered is that the most effective way to provide this defense for many customers is to provide it as a service. Instead of selling the components and trying to teach them how to use this intelligence idea, we wanted to provide it as a service. And that's a service where we go out and obtain the threat intelligence, we preprocess it, we put in place enforcement systems, we do the correlation, all the other pieces of the technology. We put that together, and so then we can defend the customer, we can actually stop the bad guy and tell the customer, you know, what happened after it's over. And customers have a problem with enough -- having enough labor and

enough people and then being trained on this new technology, effective as it is, was a bit of a stretch for them. So that's why we put together CleanINTERNET.

If I might continue --

THE COURT: Are you saying that the service would replaces the customer buying both the software and the hardware?

THE WITNESS: Yes, sir.

THE COURT: It's sort of like the Cloud in that regard?

THE WITNESS: Well, yes. If you think about it, think about the cyber thing. Companies like Raytheon and others, they have probably have 500 people doing cyber defense. How is a person like myself at my home or how are, you know, or my parents, for instance, how are they going to defend their house? How is that going to work? It's not going to work. It really needs to be a service. When you buy electricity from the power company or water from the water company, you expect to be able to drink the water, use the electricity. But when you buy Internet from the Internet company, you get criminals coming into your house. We thought the best way to solve the problem is to clean the Internet so you don't have criminals coming in your house when you use it. Does that make sense?

THE COURT: Yes.

BY MR. ANDRE:

Q. If we go to Page 5 of this document, it talks about

features and benefits of Centripetal's CleanINTERNET. Could you just briefly go over some of those features and benefits of Centripetal's CleanINTERNET?

A. Yes. So as I mentioned before, we have customers that are very big and sophisticated, they have a big team, they get this, install it and run it. But for many customers, if not most of the medium and small customers, this is what we provide in CleanINTERNET as a service. And it's a service where we install it, which goes quickly, we provide the threat intelligence, we send the threat intelligence to the enforcement point, we do the enforcement, we figure out what the bad guys are that are coming after you, we do the shielding, which is the, we protect against, you know, all this stuff coming into your network that you don't need that has nothing to do with your home or your business. We can also detect threats. So for instance if you somehow, through another means, your laptop gets infected or something, we can detect that and tell you about it and do something about it.

And then finally, we can provide compliance. There are so many compliance issues. For instance, many defense contractors are not allowed to communicate with what are called ITAR countries. Well, it's hard to keep up with those countries and what constitutes an ITAR or an entity from that country that might be in a different country. So we keep track of all that and we can help your system be compliant.

THE COURT: All right. Yesterday we were talking about on-line versus I guess we said off-line. This service functions on-line; is that correct?

THE WITNESS: Yes. All of our services actually go on-line, but some of them -- I mean, sometimes a customer will install us in a way that doesn't block, it just looks. And so then we get on the phone with them and we say, look, you're being attacked and they're stealing this information from you. In almost every case the customer says, okay, start blocking. So I think if you heard off-line, that meant we weren't blocking.

THE COURT: Well, I'm not talking about off-line, but if you used what has been described as Allow and Detect as your security system, that means that you look at what has already gone through the system and, based on a number of factors, decide whether that suggests the presence of malware. In other words, you don't -- your system doesn't function at the entrance to the Internet, it functions by examining what's already been accepted into the network system, which we talked about as Allow and Detect, which was also described as an off-line system. So that's why I ask, does it work in-line or off-line. And it sounds like what you said, it detects it in-line, and then it either blocks it or not at the option of the customer.

THE WITNESS: Well, that's mostly true. You want to stop everything that you know is bad and that you know has no

business use to the company you're protecting. So you just want to stop it.

THE COURT: Right.

THE WITNESS: On the other hand, some intelligence may be -- you're not sure about. You think it might be bad. So in that case, you might allow it into the network and then watch what it does or -- and then decide later to block it.

THE COURT: All right. Well, I understand that distinction, but that's not what I'm asking about. And I'm not sure if I'm using the right terminology, because like the law, the Internet has its own abbreviations and so forth. But what has been talked about is detecting data flow, which is after-the-fact.

THE WITNESS: You're exactly right. So --

THE COURT: Well now, does your system also investigate after-the-fact data flow?

THE WITNESS: It can do, sure. The goal is to stop the bad thing before it happens. But if it happens afterwards -- for instance, let's suppose the malware got in but it didn't come in through the network, it came in because you took your laptop down to a cafe and got infected there. So if the malware is there and the data transfer is going out, we'll detect it on the way out and stop it, if we can, going to the place it's not supposed to go. So yes, I think the answer to your question is yes.

THE COURT: Well, okay. Now, so but you don't rely on data flow as an integral part of your system? That's sort of an extra or and add-on; would that be accurate?

THE WITNESS: Well, it's an important add-on. But I would say that if you're doing cyber defense, the thing you most want to do is to stop it before it ever gets in your network or never happens.

THE COURT: Wasn't it part of the problem that you were trying to solve that measuring data flow after it already entered the network was an after-the-fact solution, and you were looking for a solution that would prevent it from getting into the network in the first place because after-the-fact solutions weren't working? Isn't that what you were trying to do?

THE WITNESS: Exactly right. In fact, when you hear about a cyber breach -- for instance, we just heard a week ago about a big breach of Marriott and all their customer accounts. What happened was they discovered that the attack had happened, but unfortunately they discovered it long after all the data was gone. And that's the way most cyber defense is still to this day.

THE COURT: All right. I think you've answered my question.

BY MR. ANDRE:

Q. So Mr. Rogers, and just to clarify, the technology you deployed in the market, could it be deployed in-line and

out-of-band?

A. Both ways, yes.

Q. Okay. And when you use threat intelligence, that second bullet point on the slide there, over 90 integrated threat intelligence providers, now, could you explain where you get your threat intelligence from?

THE COURT: Would this be a good time to adjourn for lunch?

MR. ANDRE: It would be, Your Honor.

THE COURT: All right. We'll be in recess until 2:00.

MR. ANDRE: Thank Your Honor.

THE COURT: During the recess, Mr. Rogers, you should not discuss your testimony with anyone or review any documents. You should return to your testimony with the same level of knowledge as you currently possess.

THE WITNESS: Yes, sir.

THE COURT: All right.

(Luncheon recess taken at 12:59 p.m.)

CERTIFICATION

I certify that the foregoing is a true, complete and correct transcript of Volume 2A of the proceedings held in the above-entitled matter.

Paul L. McManus, OCR

Digitally signed by Paul L. McManus, OCR
DN: cn=Paul L. McManus, OCR, c=US, email=pmcmanusocer@verizon.net
Date: 2020.08.10 10:28:49 -04'00'

Paul L. McManus, RMR, FCRR

_____

Date